Help Center

Phison - Double block rotation and SLC block management

The solution step by step

It’s been many years since the first NAND controllers were released on the market. Many technological aspects of flash devices have changed since that time, but one thing is certain, along with the multiplied capacity, the quality of data inside NAND chips has been decreased significantly.

Therefore, controllers are using many sophisticated functions to protect stored data. We can observe these results during our daily work, many steps have to be applied before data will be recovered and almost every operation, we reverse, is applied to protect user data as well as possible.

In this article, we would like to bring closer SLC blocks topic and present to you the solution for Phison controllers which are using double rotation mode.

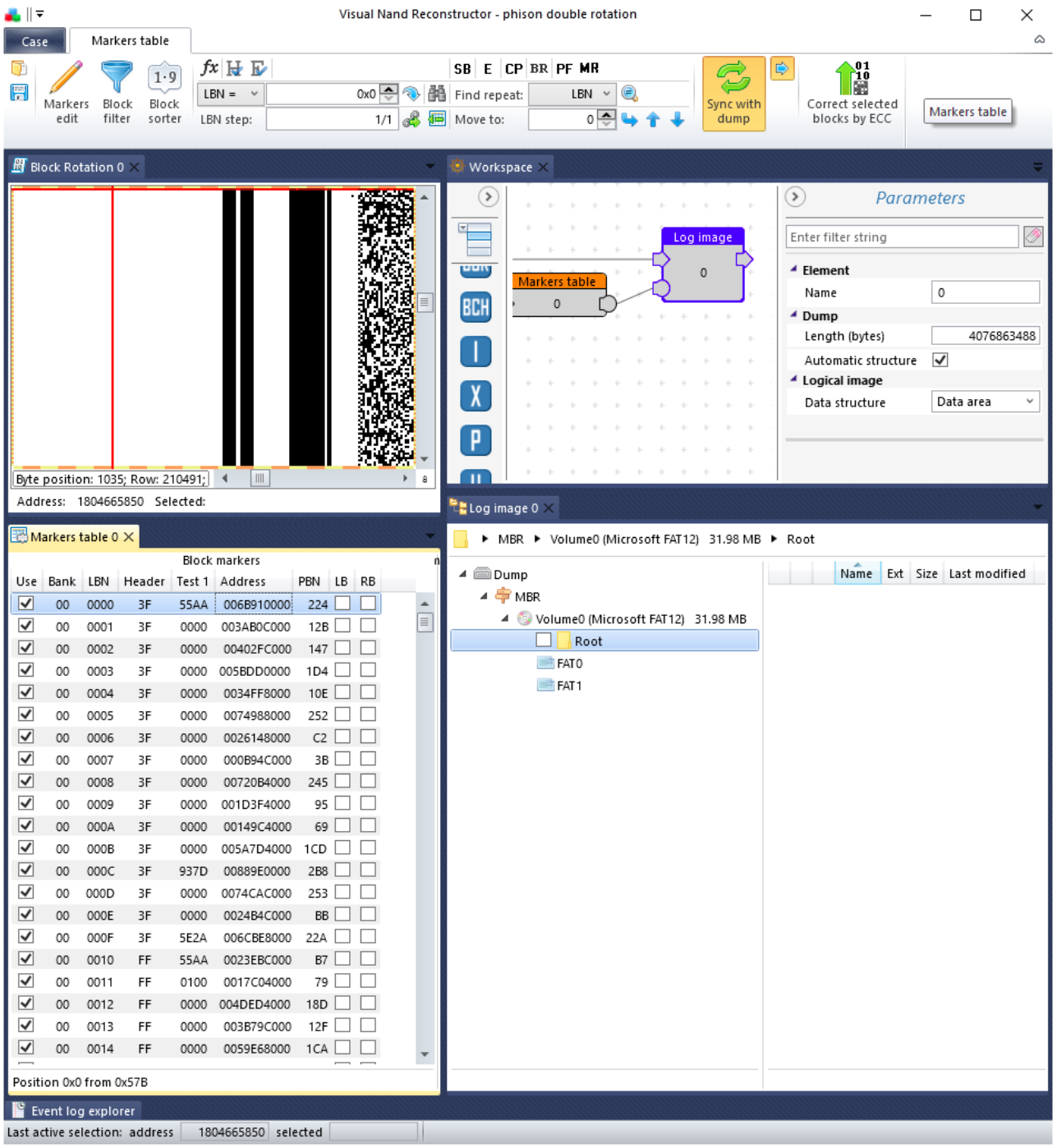
How to recognize that controller uses double rotation?

How to reverse this type of rotation?

How to pull out data from the SLC block?

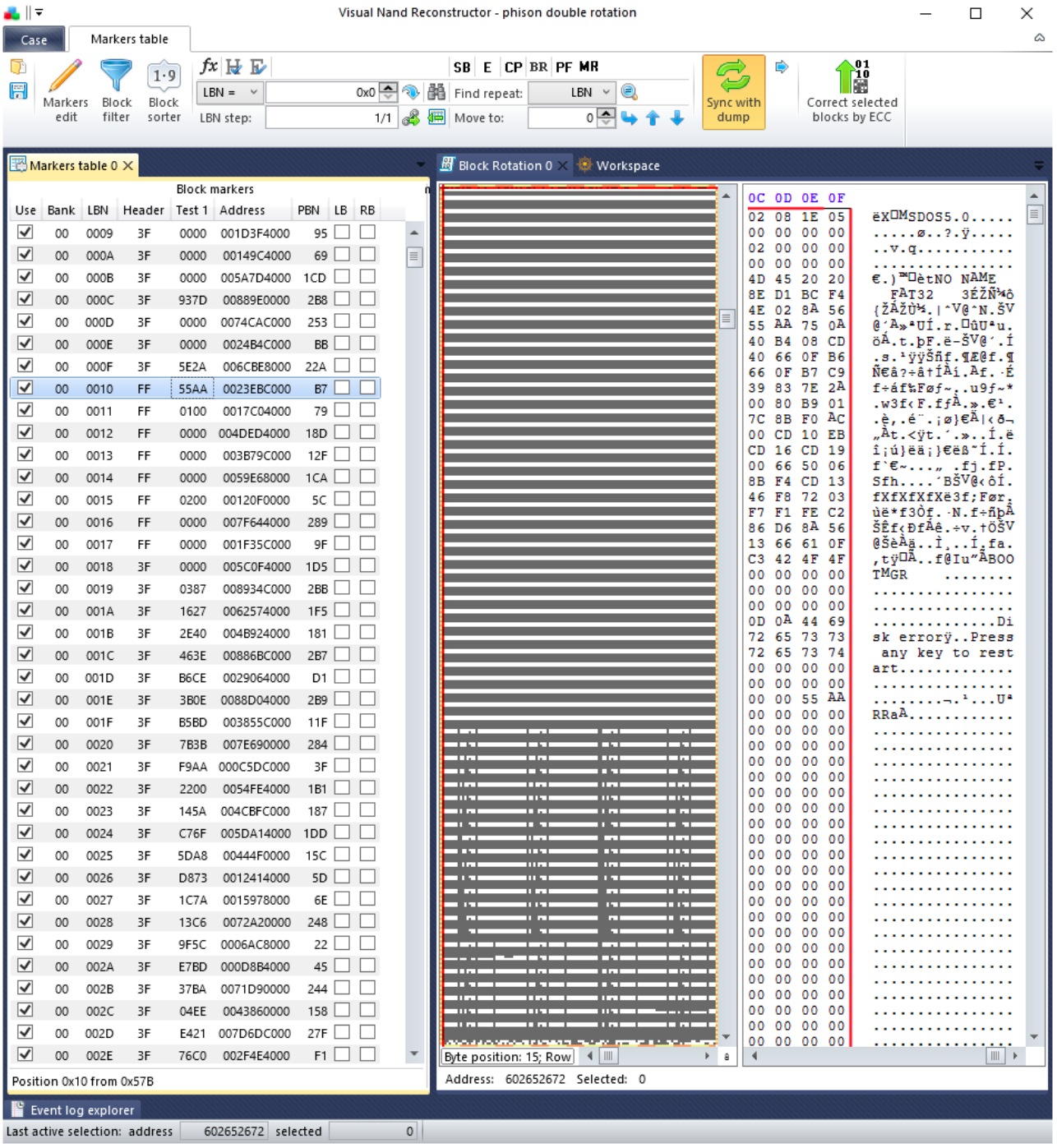
All this information you will find in this article.

In the example below we have a dump from a micro SD card equipped with a Phison controller. We’ve used static rotation, but despite, that the rotation element is attached, we could not access the file system.

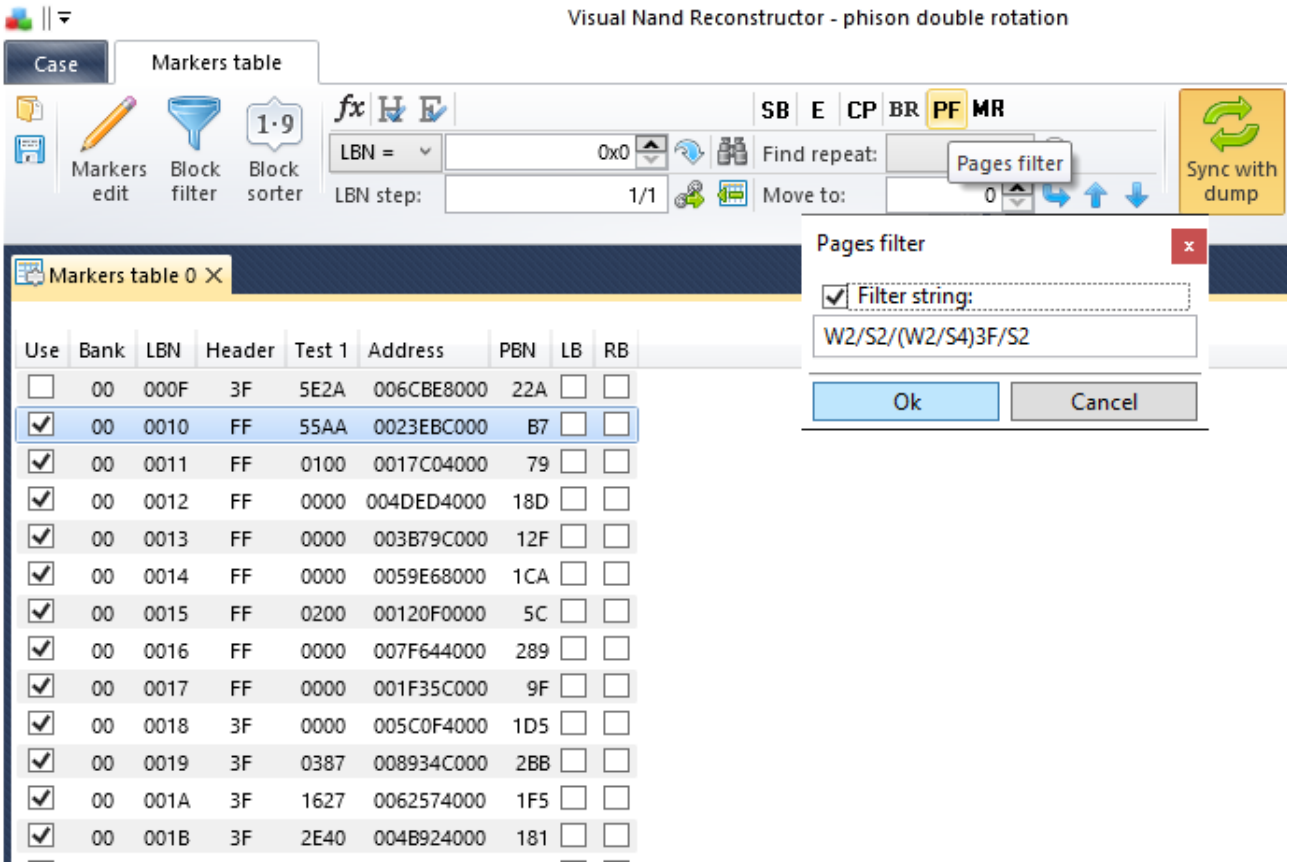


Block with LBN 0000 has MBR signature (55AA) on the bytes position [510,511], the same signature has block 0010, it has a boot sector and contains a part of the FAT table and this particular block can be used as the first one, so the beginning of the logical image.

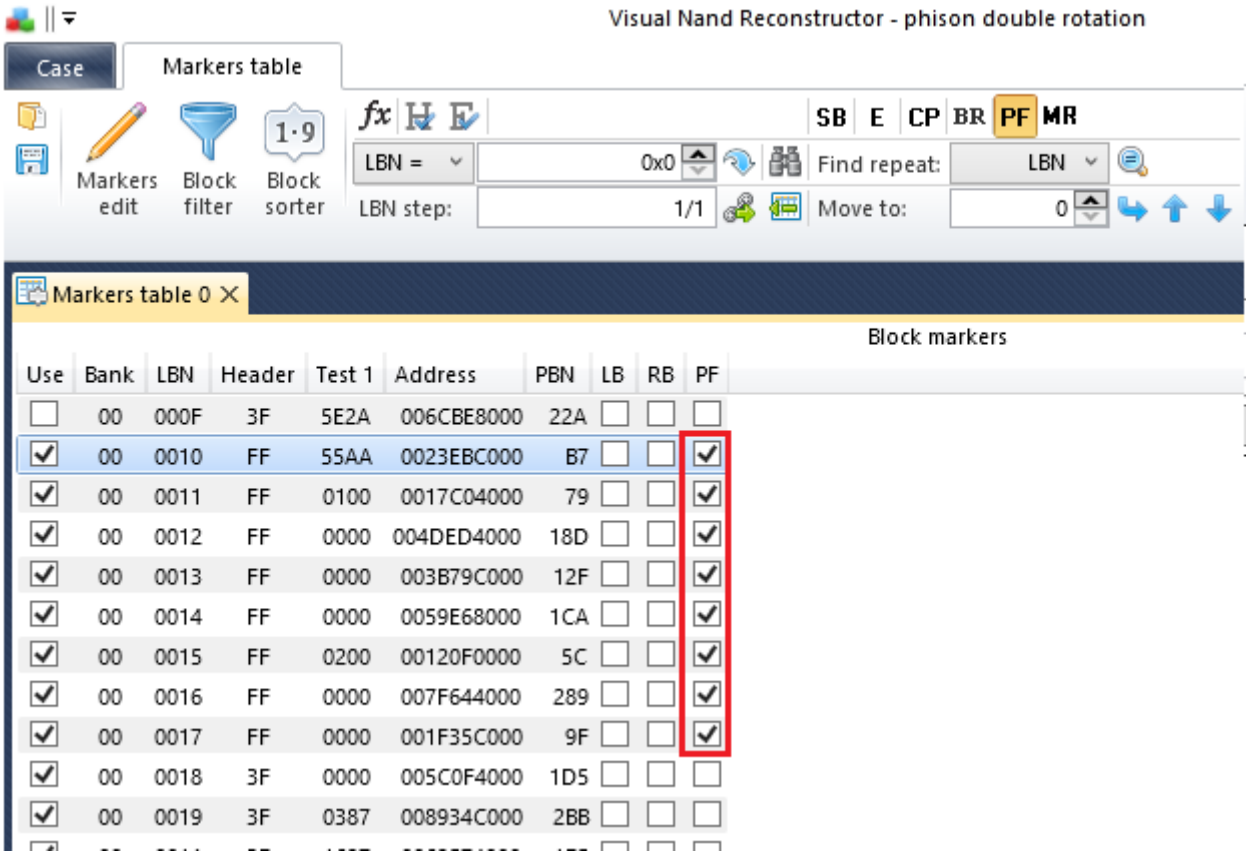
This particular block also has a very specific pattern, we can say it has “stripes” in fact these are alternating pages with data and empty ones(0xFF). This is the so-called “SLC block” of MLC memory and only SLC pages are used by the controller. Pages without data, so MLC ones should be simply filtered out.



To filter out empty pages VNR has a built-in tool inside the Markers Table element called “Page filter”, to use this option it is necessary to click the “PF” icon and input the appropriate formula.



When the formula has been added in the Markers table new column will appear and it will be necessary to tick all SLC blocks on which filter should be applied.


Visual Nand Reconstructor - phison double rotation
Case
Markers table
Markers edit
Block filter
Block sorter
SB E CP BR PF MR
LBN =
0x0
LBN step:
1/1
Find repeat:
LBN
Move to:
0
Markers table 0
Block markers
Use Bank LBN Header Test 1 Address PBN LB RB PF
00 000F 3F 5E2A 006CBE8000 22A
00 0010 FF 55AA 0023EBC000 B7
00 0011 FF 0100 0017C04000 79
00 0012 FF 0000 004DED4000 18D
00 0013 FF 0000 003B79C000 12F
00 0014 FF 0000 0059E68000 1CA
00 0015 FF 0200 00120F0000 5C
00 0016 FF 0000 007F644000 289
00 0017 FF 0000 001F35C000 9F
00 0018 3F 0000 005C0F4000 1D5
00 0019 3F 0387 008934C000 2BB

Let’s back to the page filter formula.

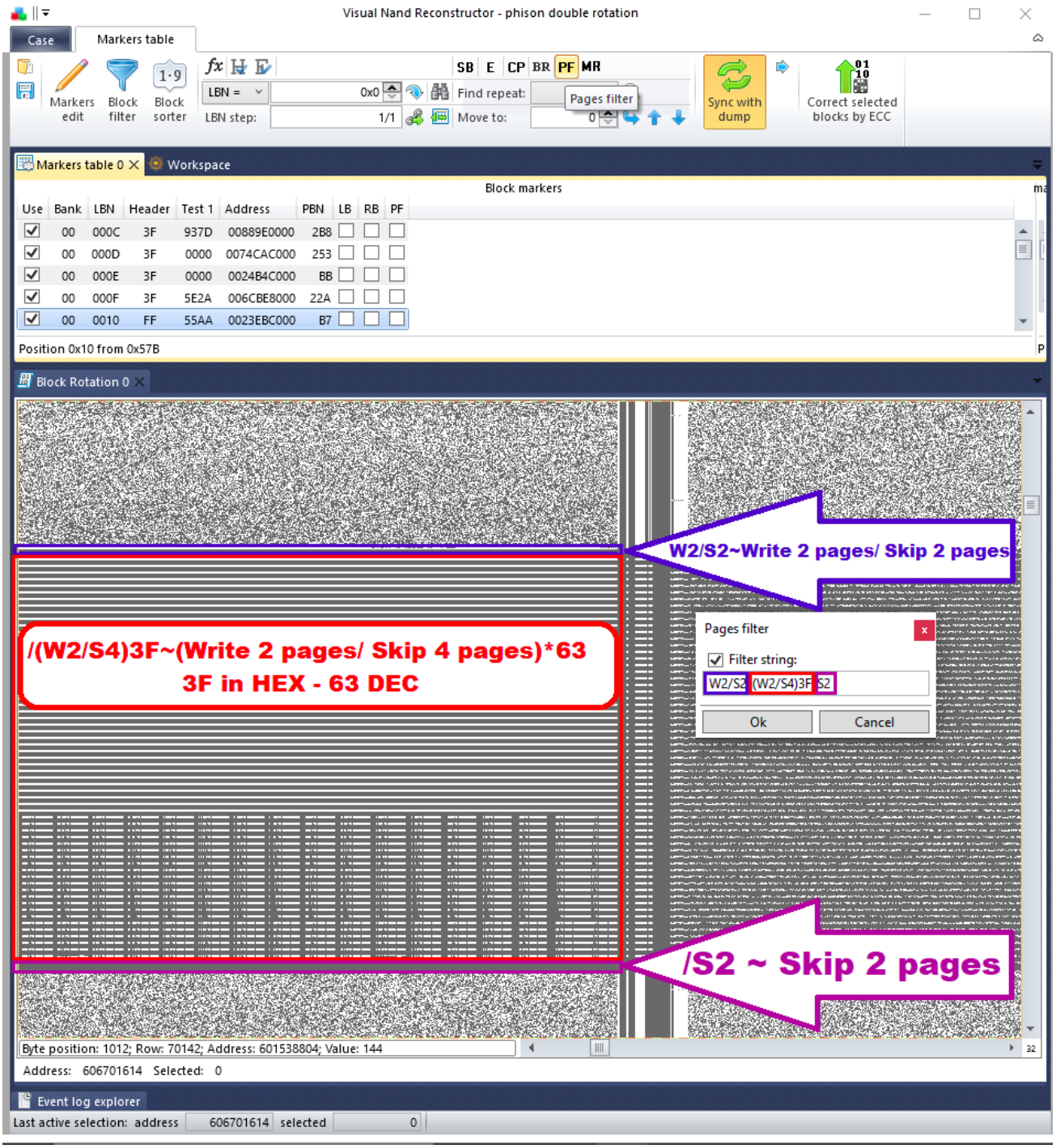
Numbers in the formula should be precise in Hexadecimal values plus two key marks “**W**” and “**S**”.

W – WRITE/TAKE
S – SKIP

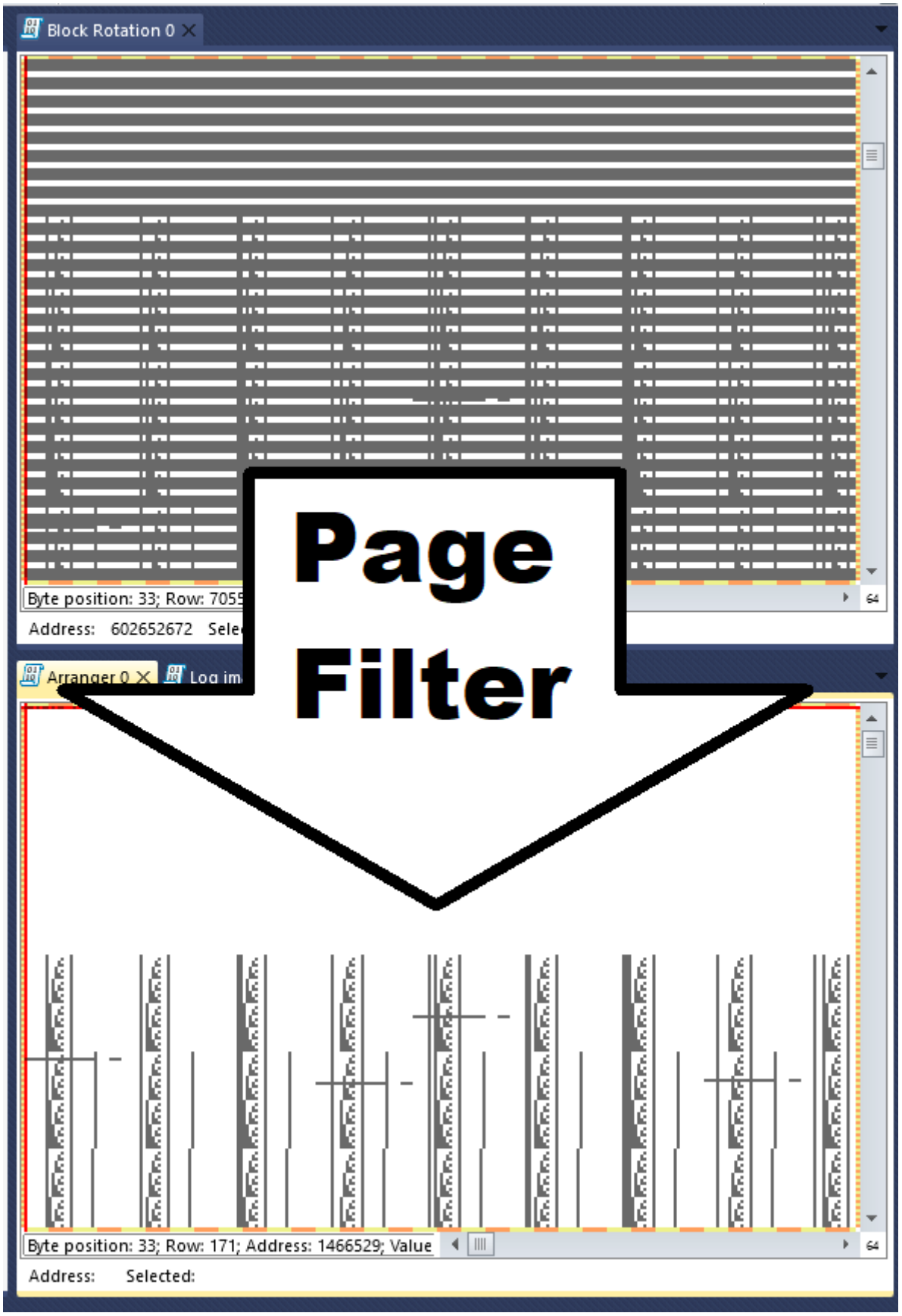
Formula W2/S2(W2/S4)3F/S2 means:

Write/Take 2 pages, skip 2 pages, (write 2 pages, skip 4 pages) *63, skip 2 pages.

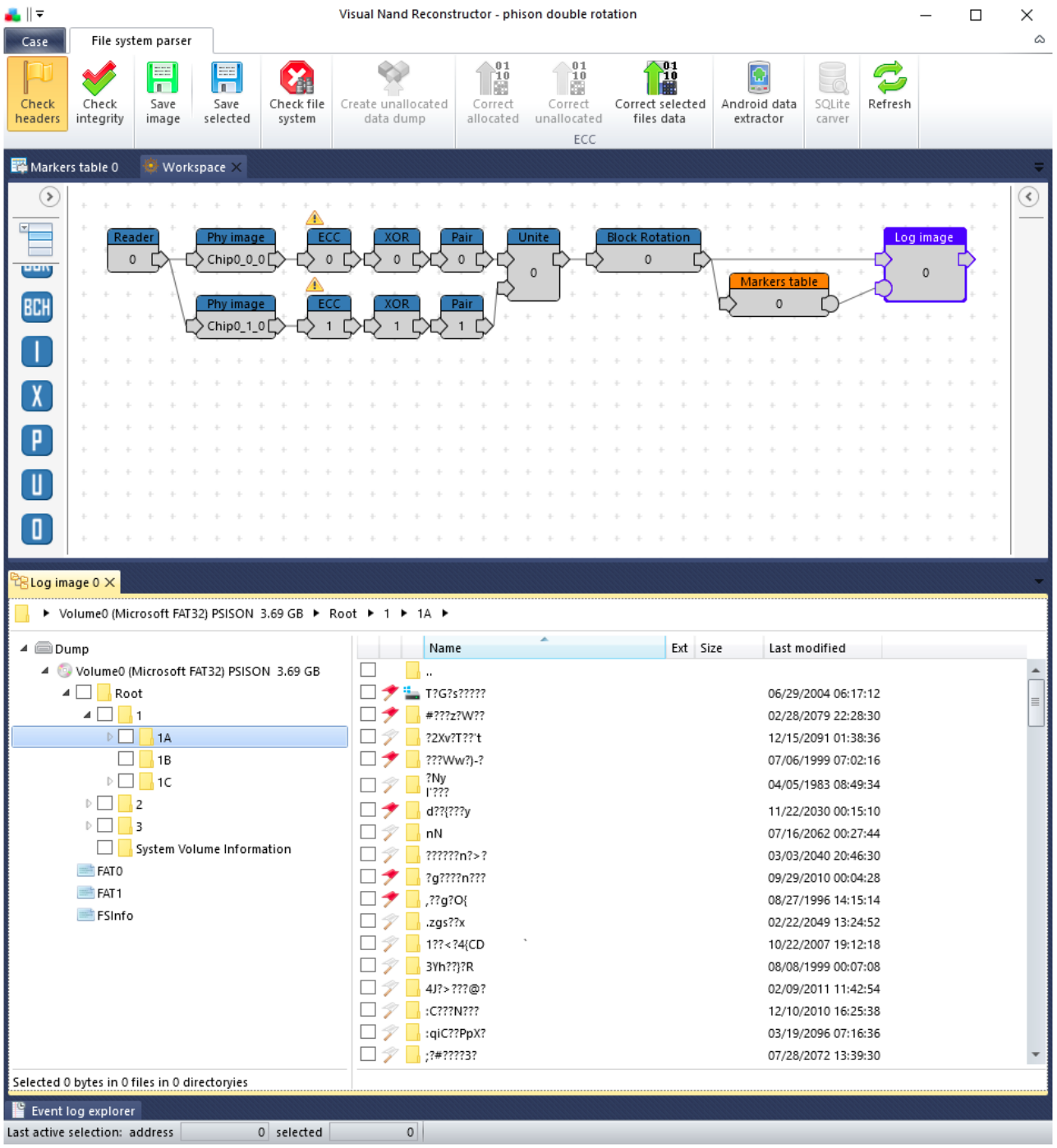
The important thing- the formula depends on the Chip and controller



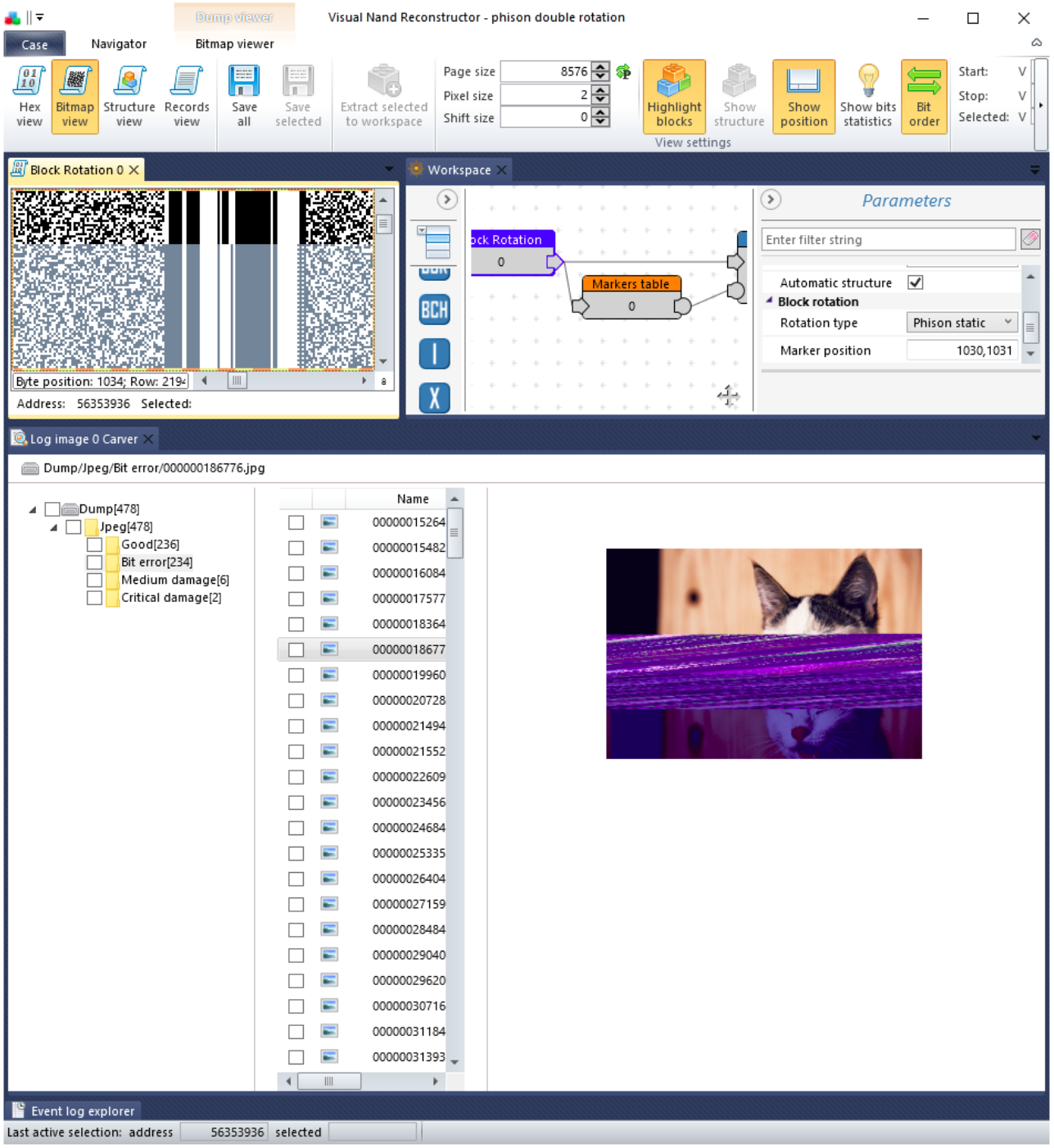
Page filter can extract necessary pages and here is an example of how it works:



In this case, even if we have used the page filter, the file structure is still unavailable:



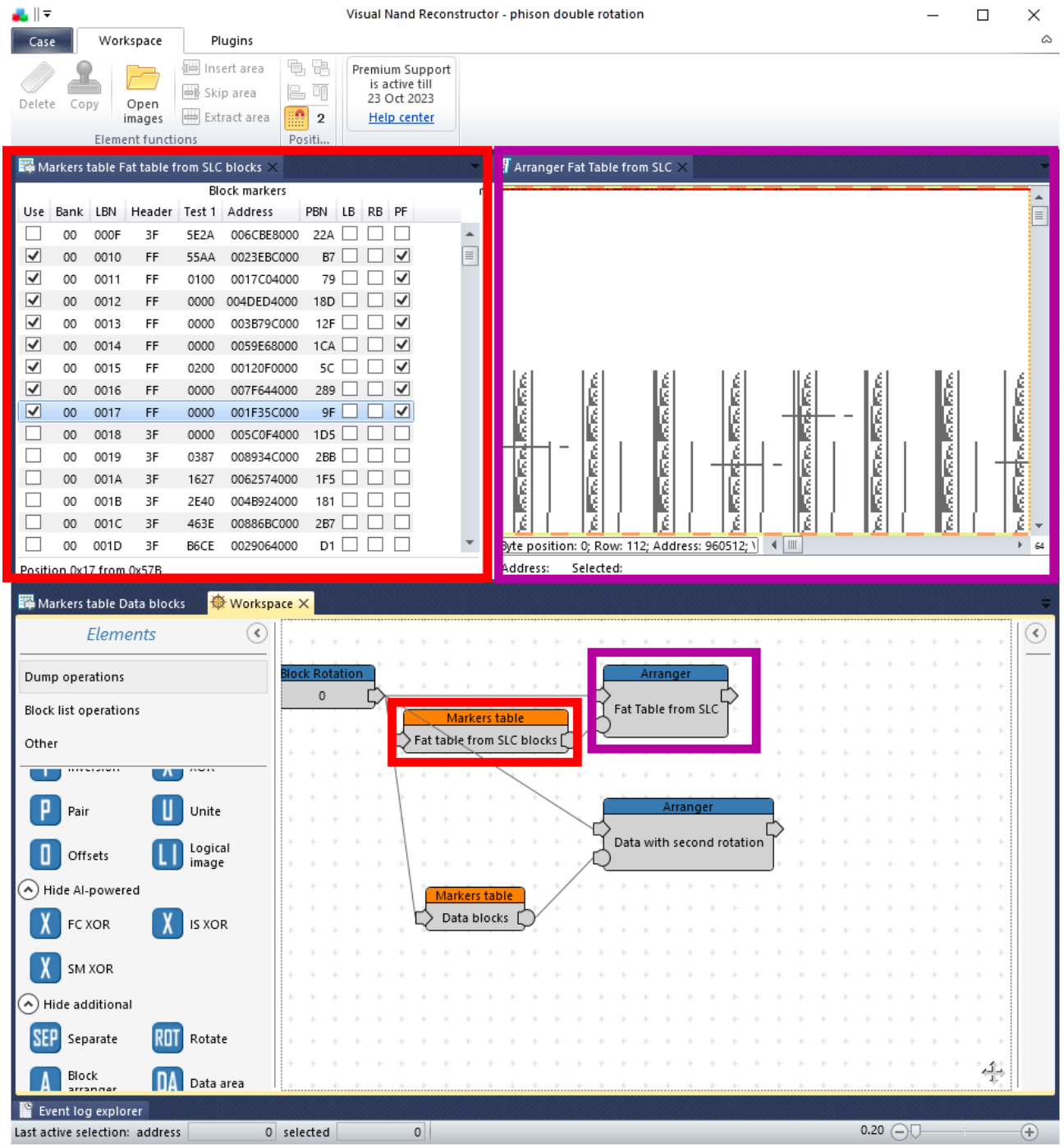
After scanning the logical image by file carver we still have damaged files, despite the use of the block rotation element.



We've reached the key point and found the reason why files are damaged. The device has double rotation and to reverse it will be necessary to assemble the image by offsets and use a new option in concatenate element.

First of all, we should separate SLC blocks. For this purpose, we can use the Markers table, with selected SLC blocks only, and connect the Arranger element.

!NOTE:
This type of block does not contain double rotation, so any additional element isn't required.



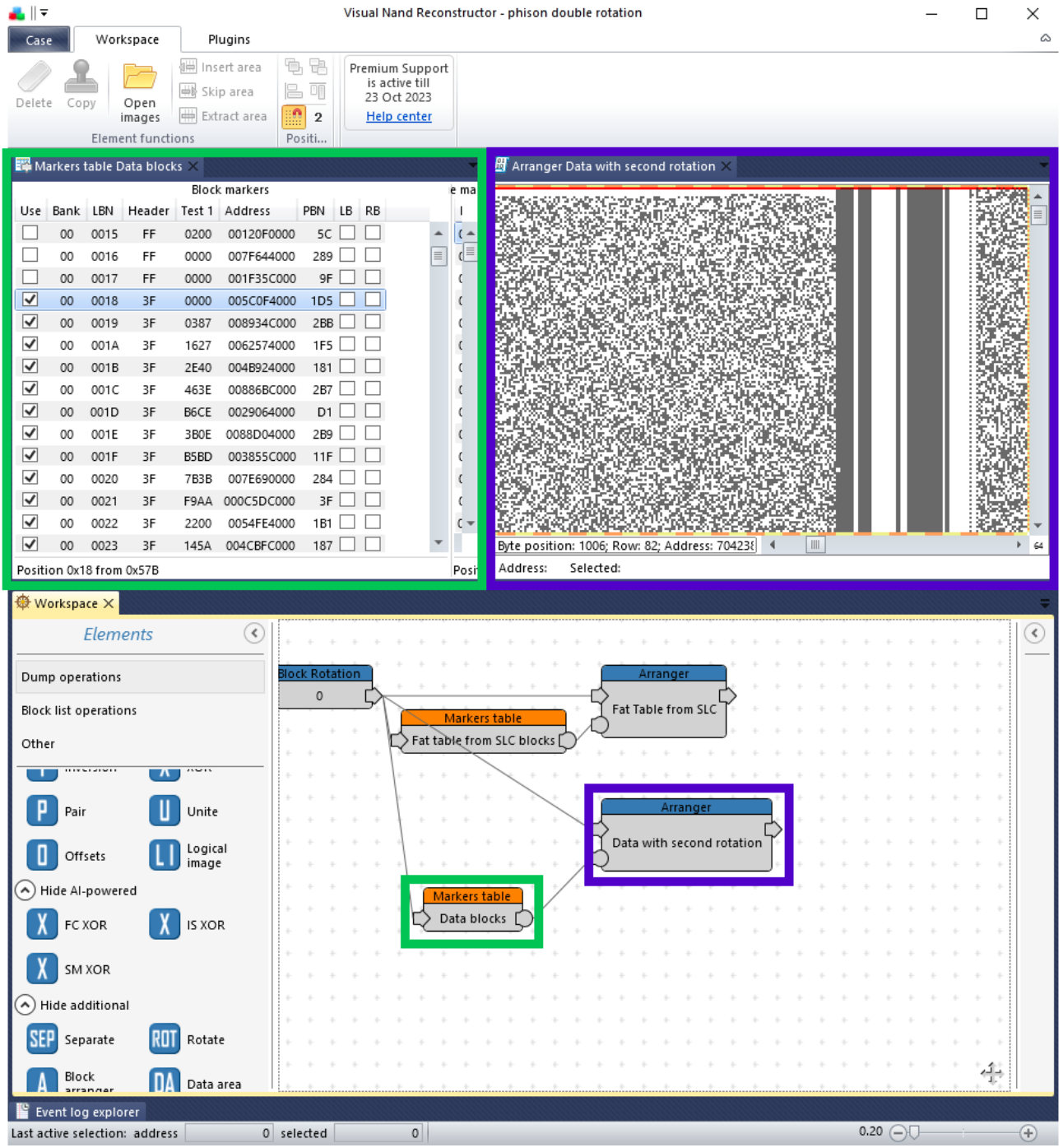
The second markers table should contain only normal blocks, so non-SLC blocks.

These blocks should be sorted and their LBN chain should be fixed, so we shouldn’t have any duplicated blocks and afterward, it’s necessary to insert missing blocks, so the same approach for Markers table like for the other simple cases.

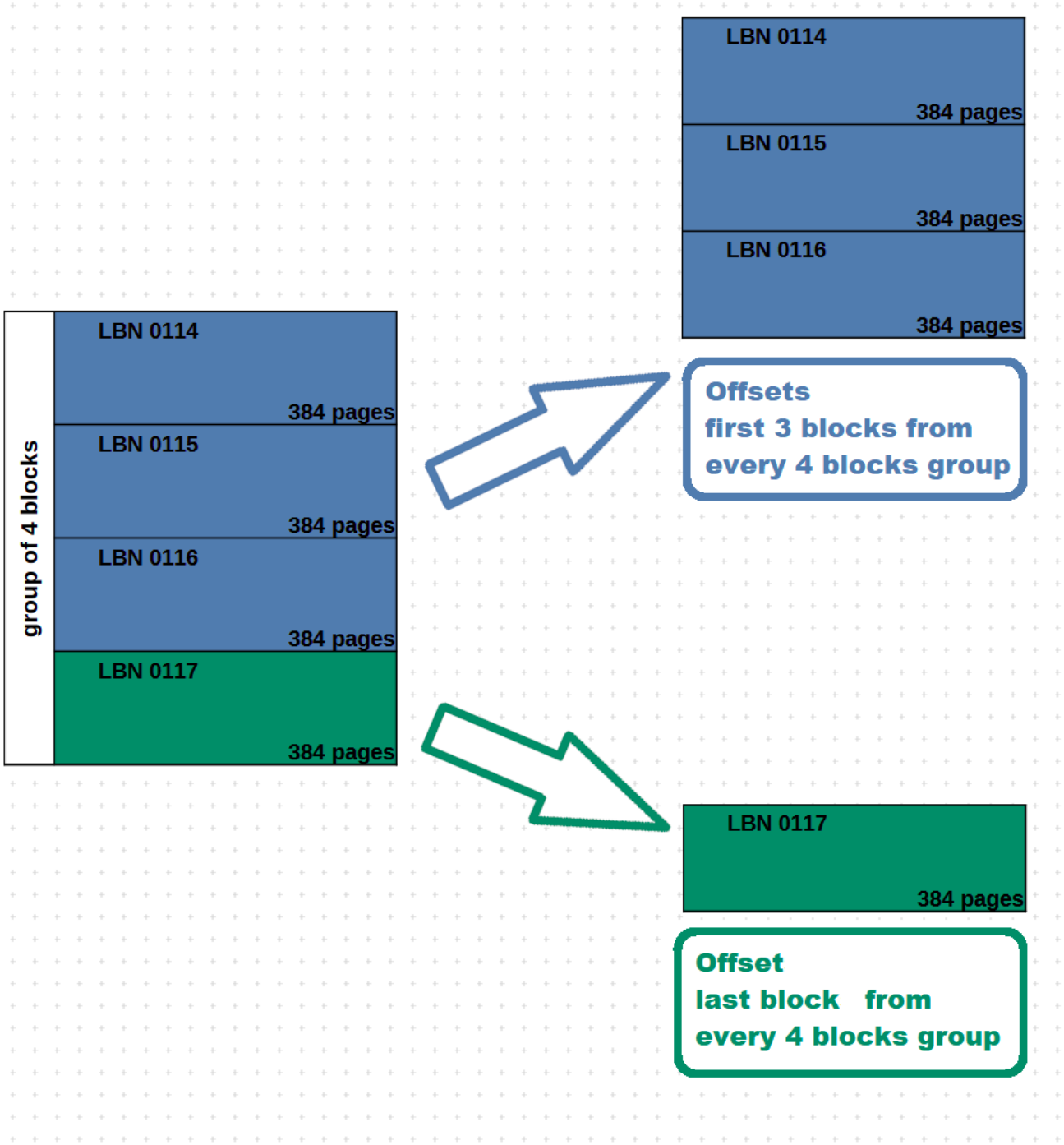
The number of selected blocks in the Markers table has to be divisible by 4, otherwise, it may not be possible to apply further operations. The number of blocks can be checked in the Markers table, **check block Position.**

So the last block from the first block table was 0017, and in this block table, the first one will be 0018.

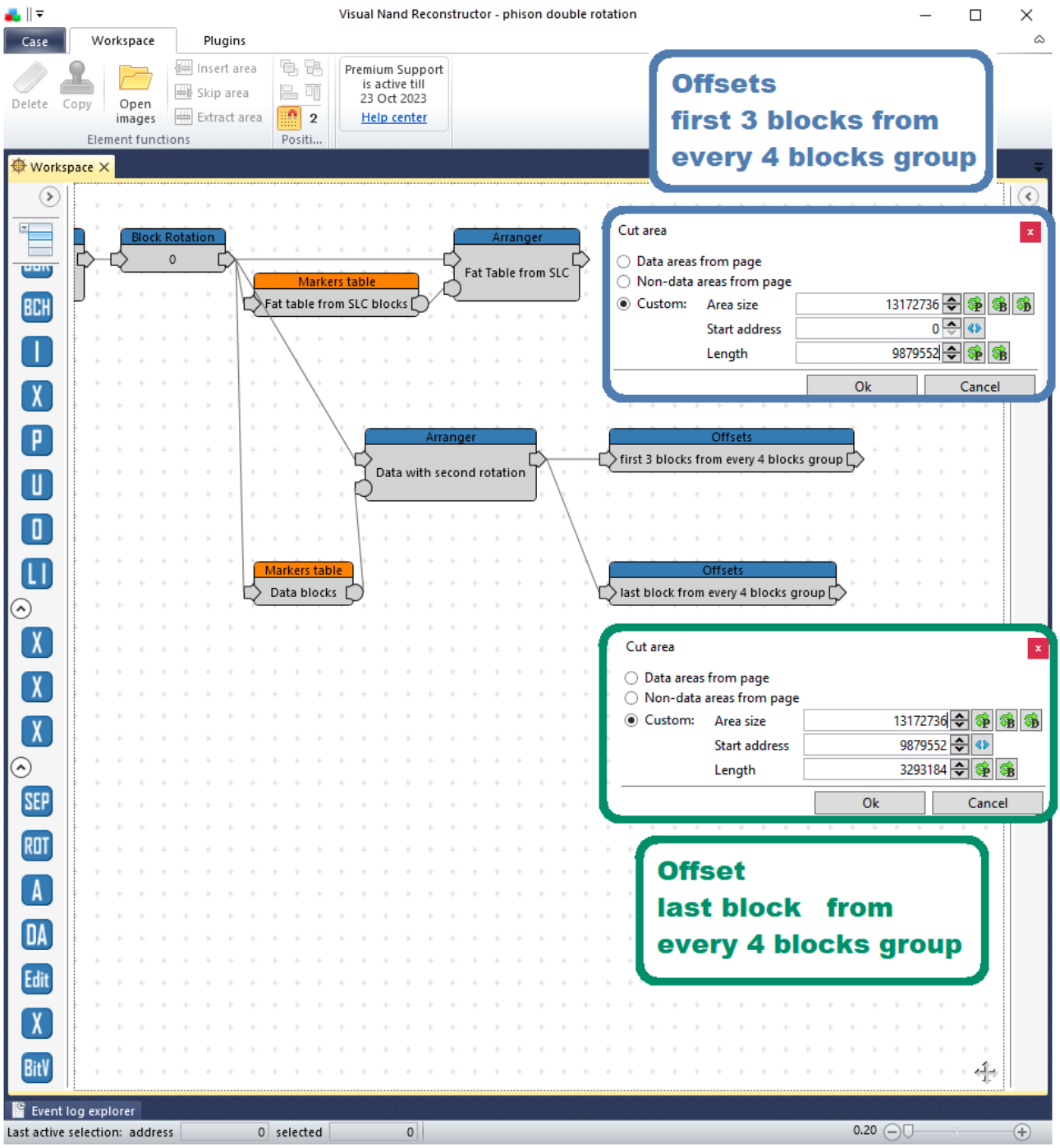
The last block should be **XXX3, XXX7, XXXB, XXXF.** That rule can help us to get the number of blocks divided by 4.



When all data blocks are inside the arranger, it is necessary to make the offsets, and rule how to do this is not difficult. There are groups of four blocks.
The first step is to extract two offsets.
In the first offsets, we have the first three blocks from every one group, in the second offset, there are the last blocks only from every one group.

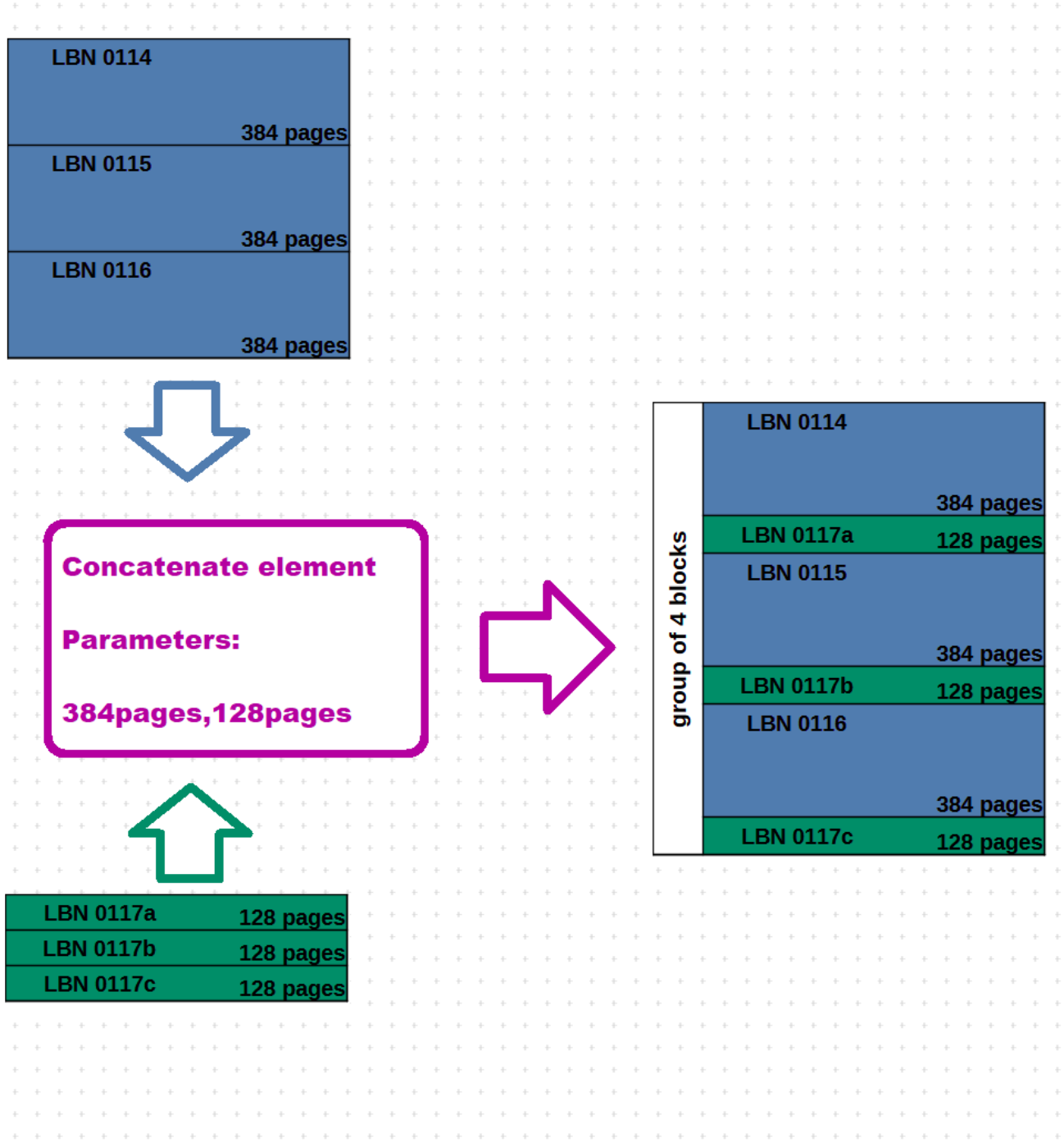


That’s how it presents in the case:

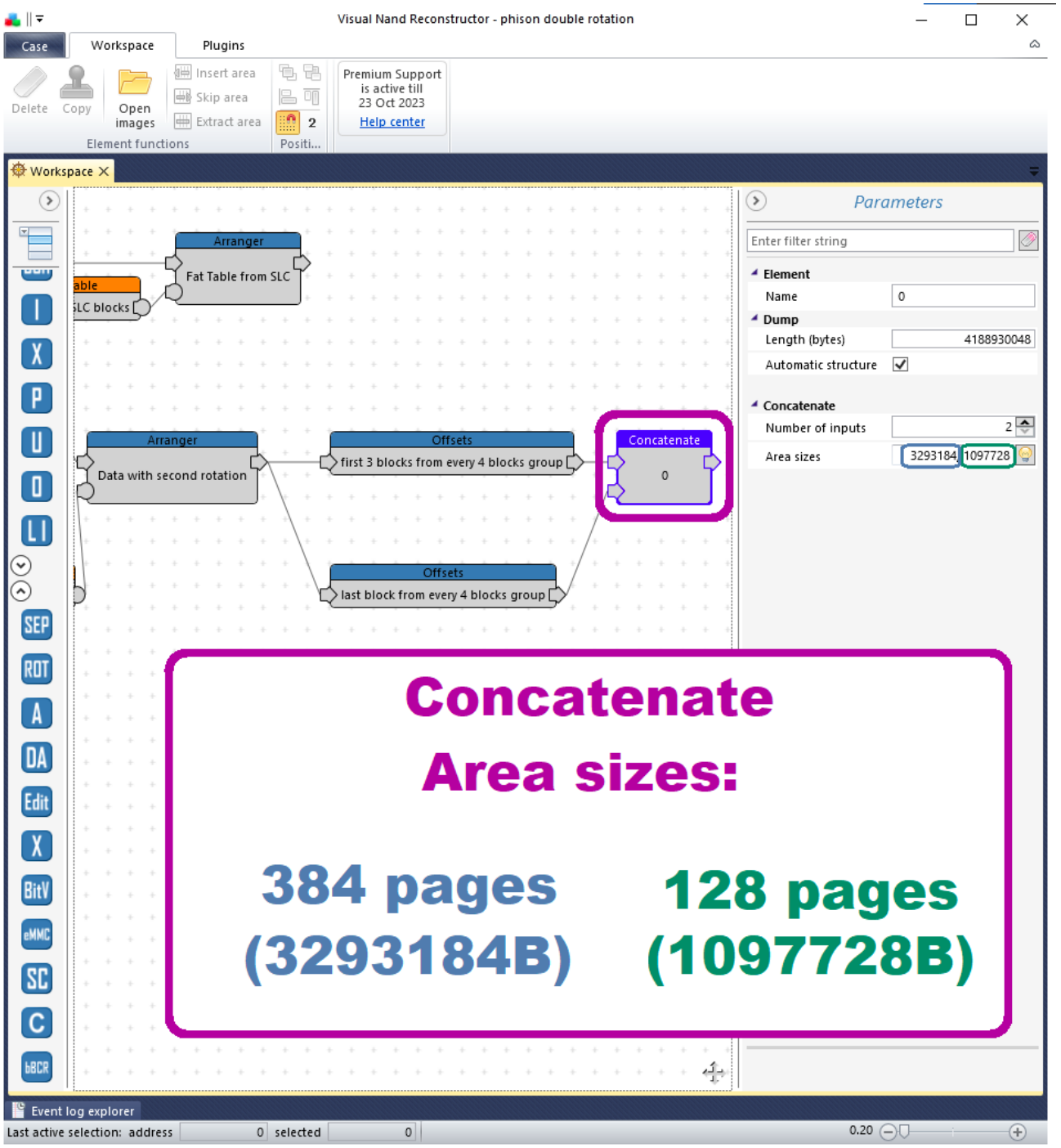


In the next step, it is necessary to concatenate offsets by parameters.

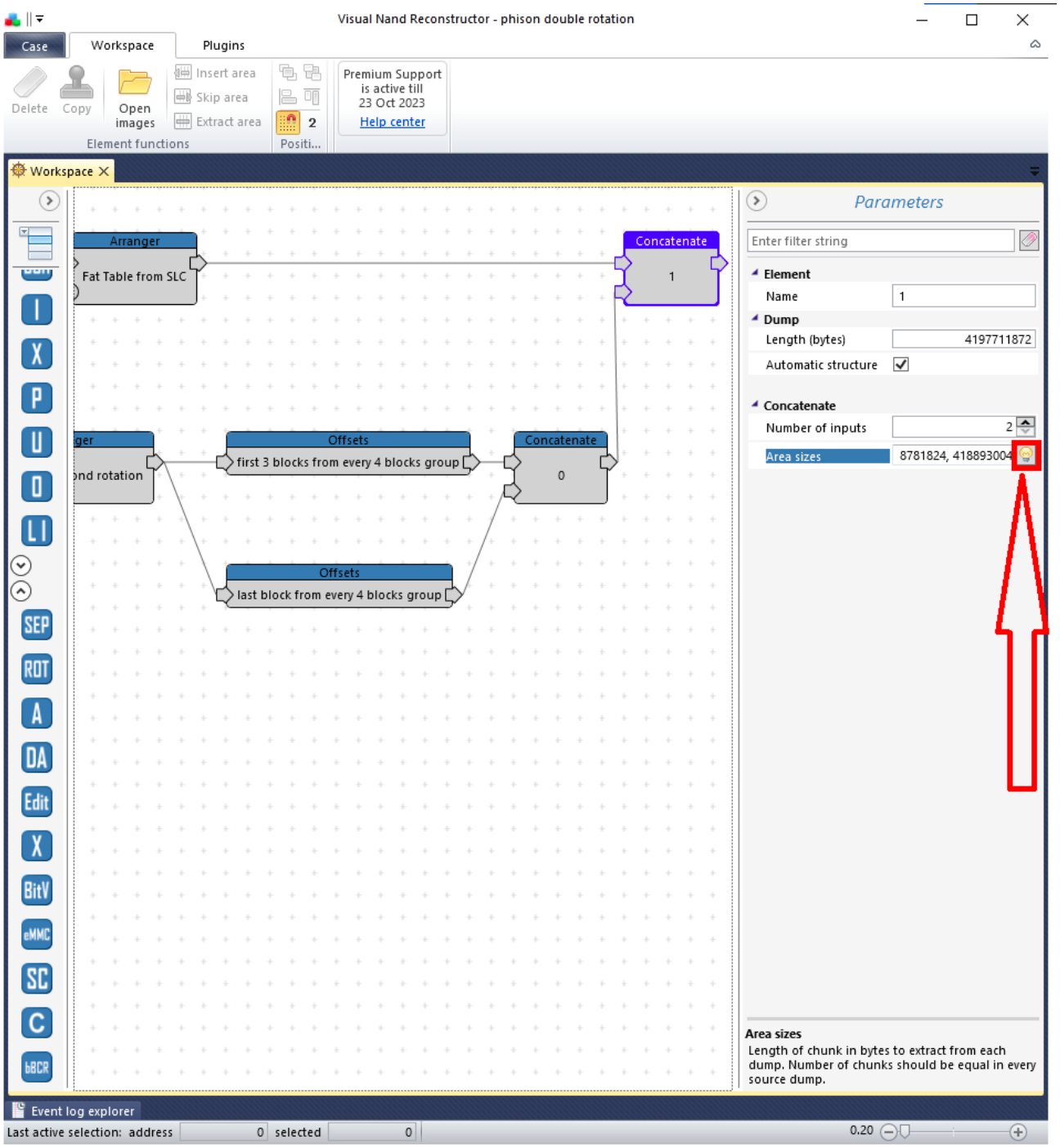
The last block from every group is divided by three and those small chunks are added to the first three blocks in the group:



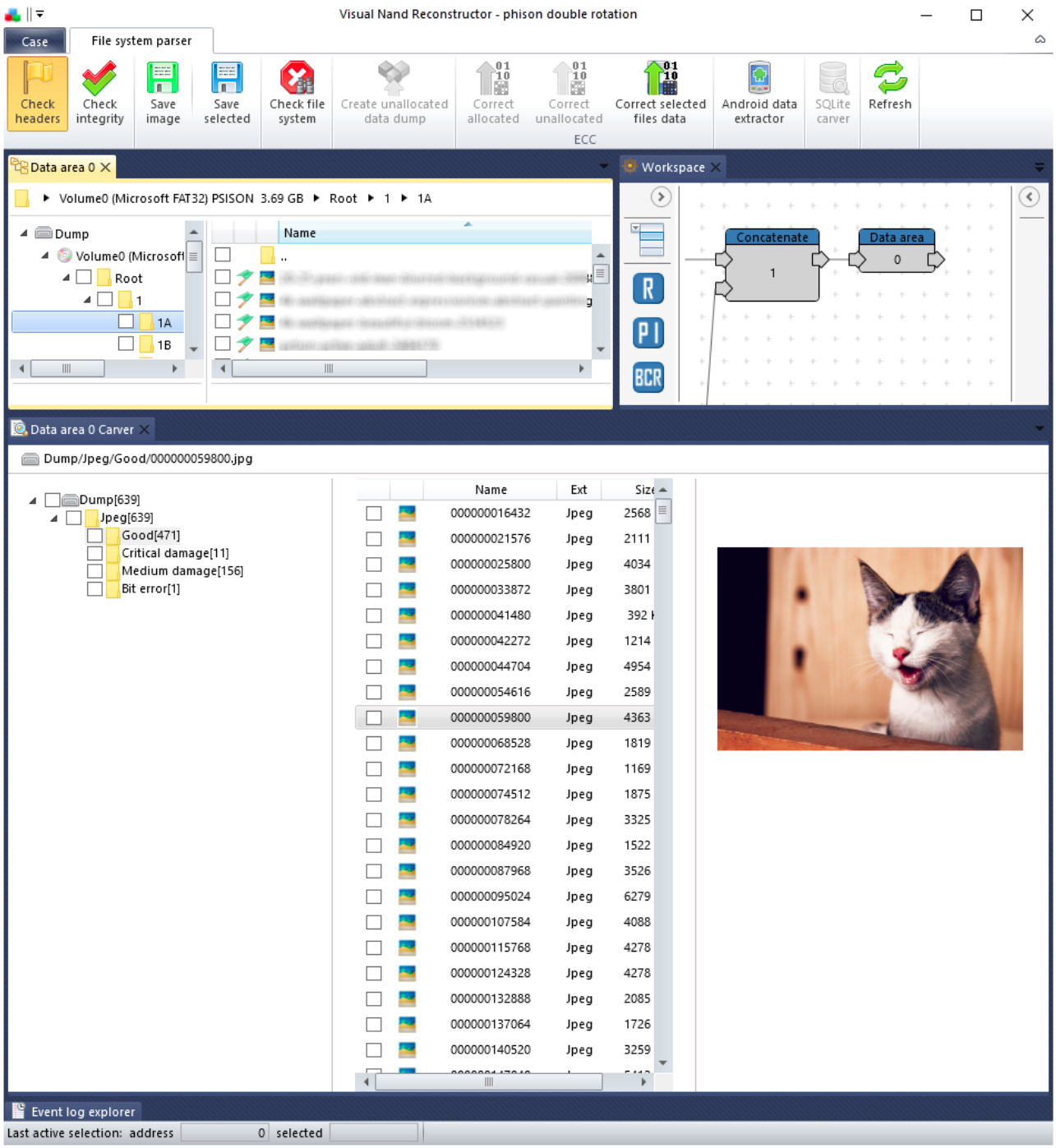
The most important are Area sizes:



In the next step, SLC blocks should be joined with the other remaining blocks. For this purpose, the additional concatenate element should be used. Click on the bulb icon to extract area sizes. So then two dumps will be joined by whole sizes one after another like a simple JBOD.



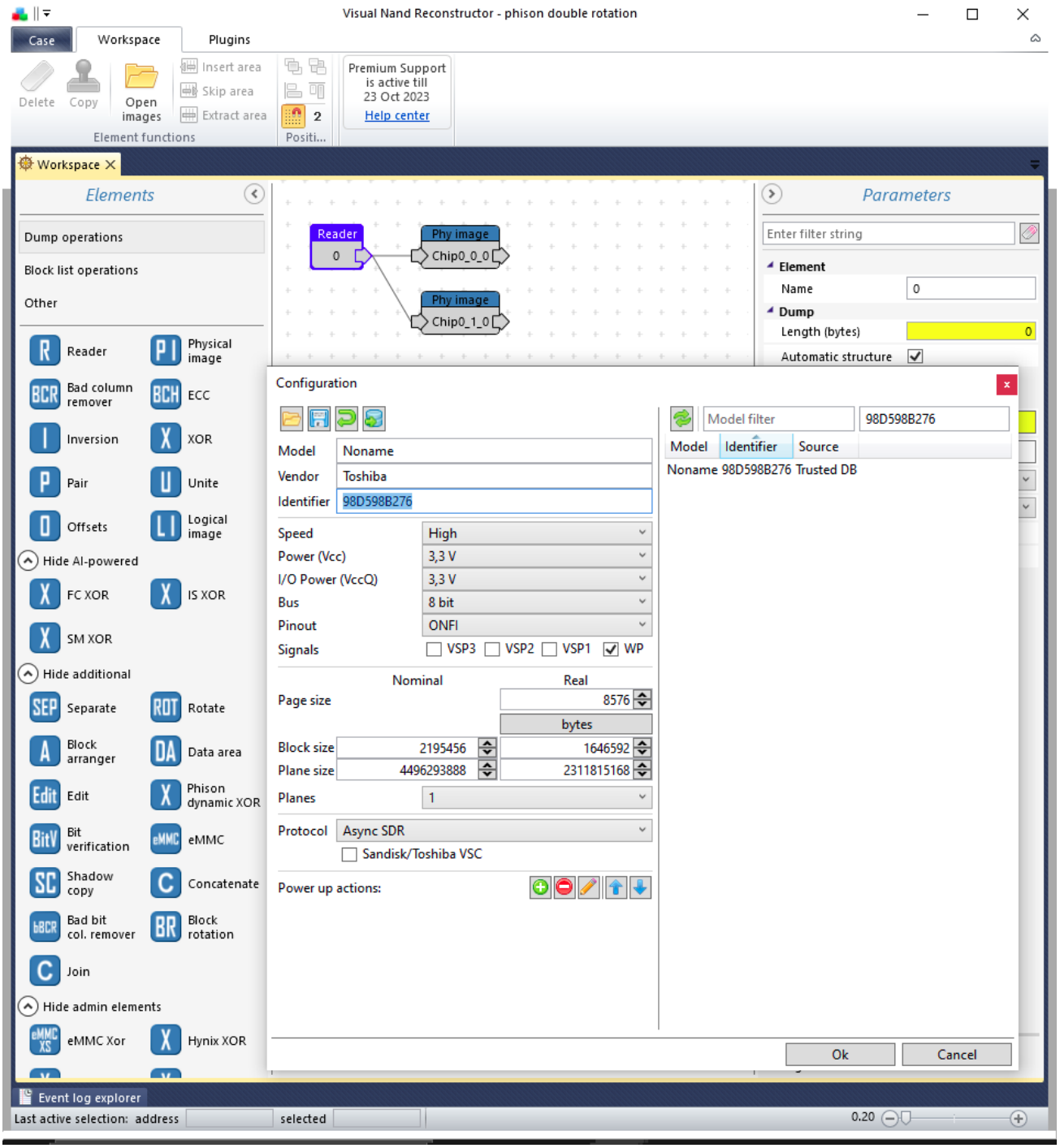
After this operation, all blocks are ordered properly, so in the last step, the data area element will be required to pull out the logical image.



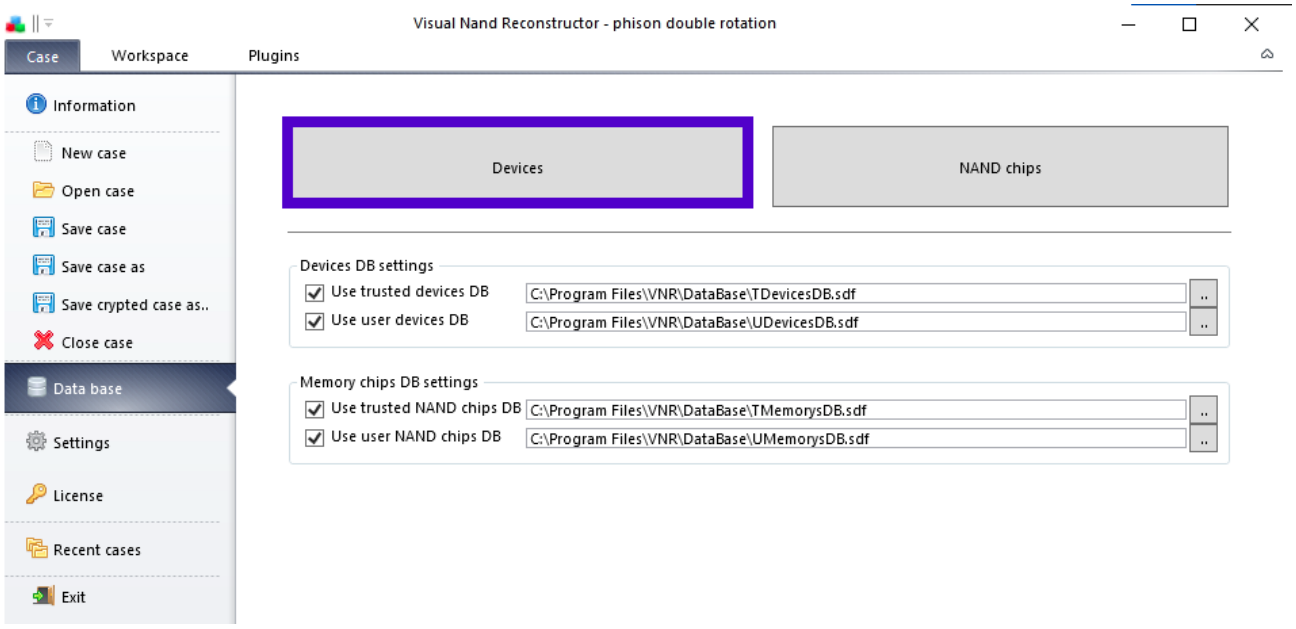
The solution from Device Database:

It is a very complicated case to solve, but that kind of solution we have found only with one ID, and now there is a faster way to solve it, all that is necessary to do is check this ID in database "Devices".

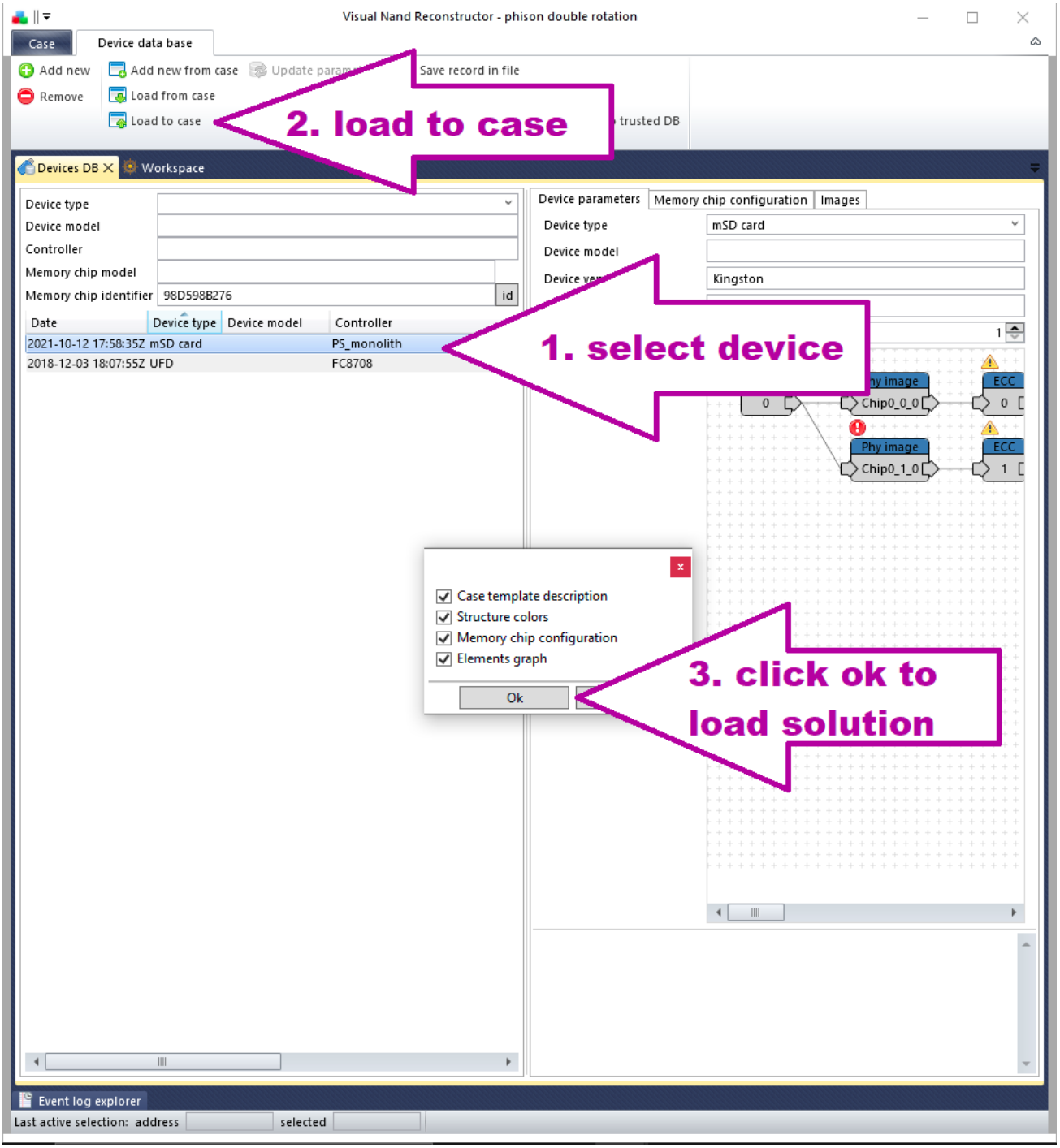
The first step is to copy the ID:



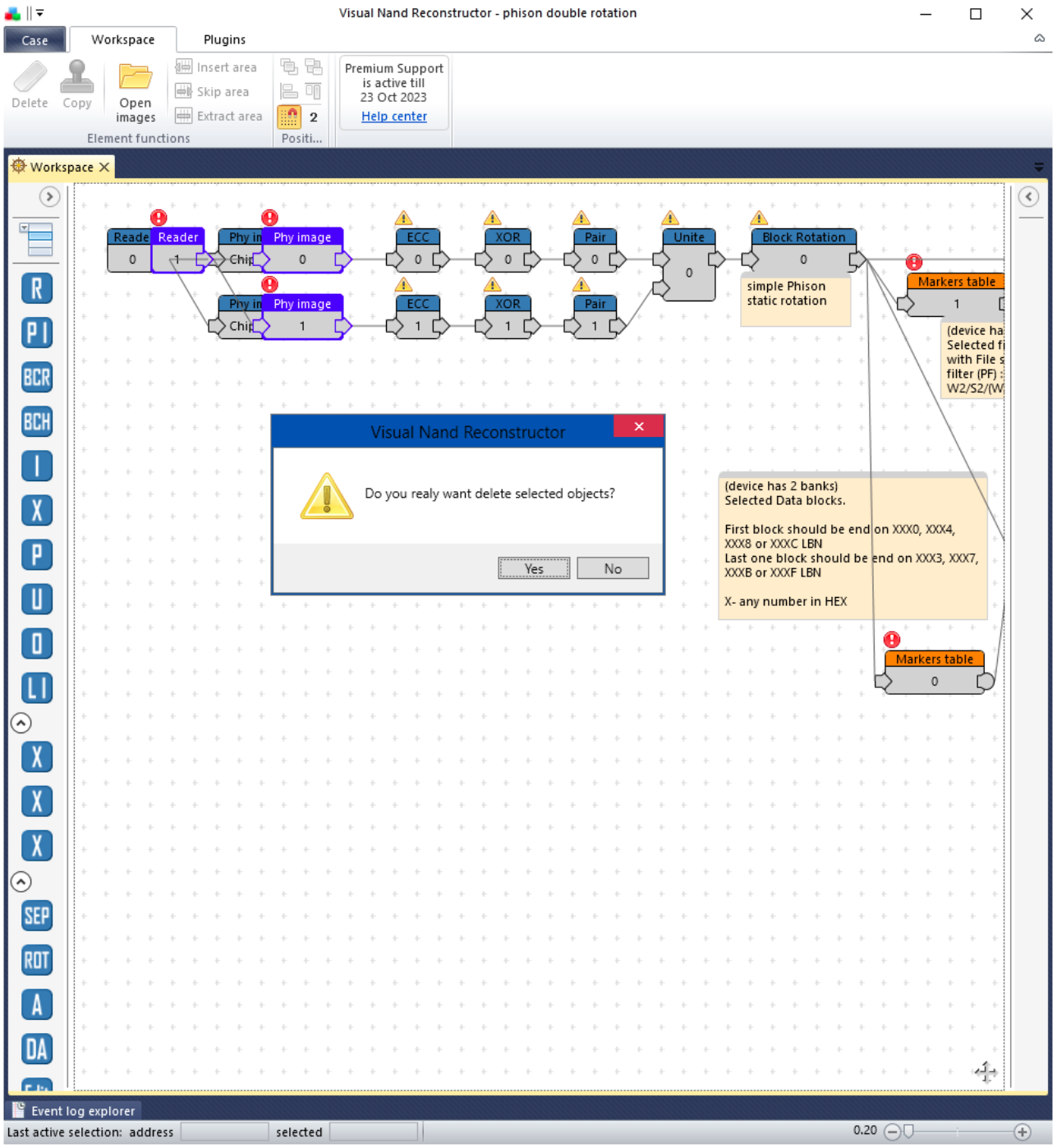
The next step is to open the Devices Database:



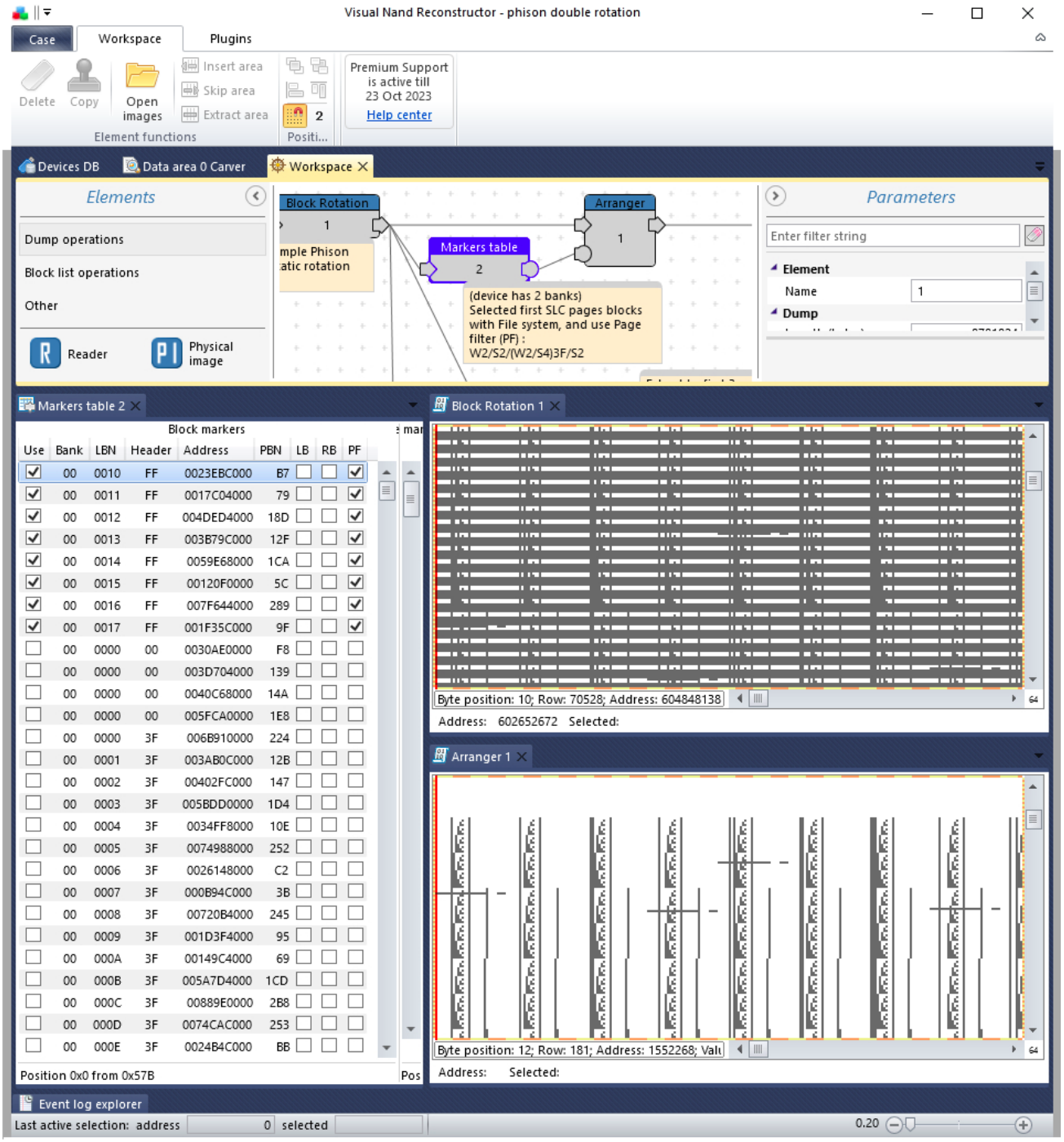
If there is the same device in the database, we can load the solution to the case:



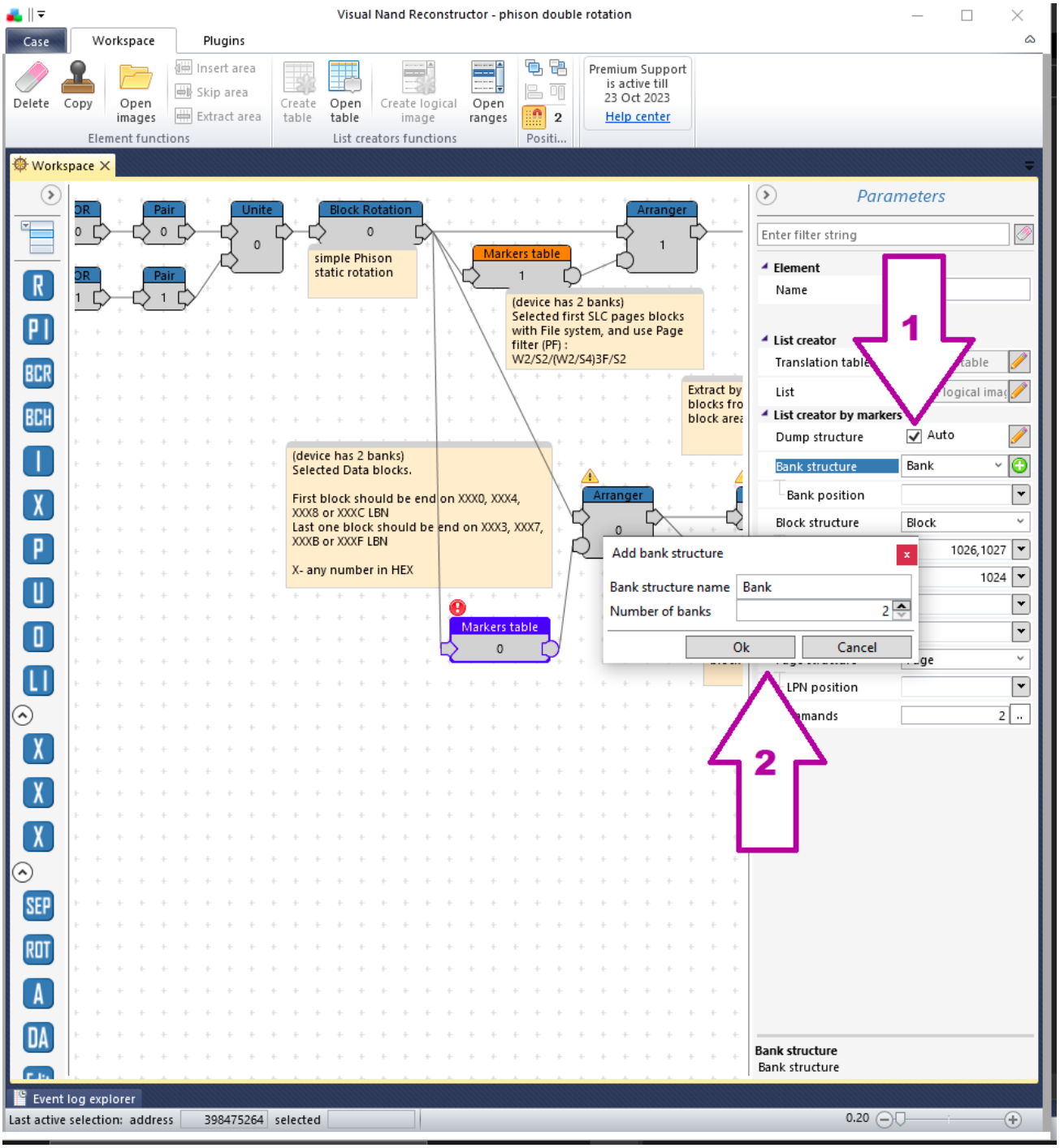
After that operation, all elements are inside the Workspace, after that it is good to remove the repeated elements and then to connect graph elements.



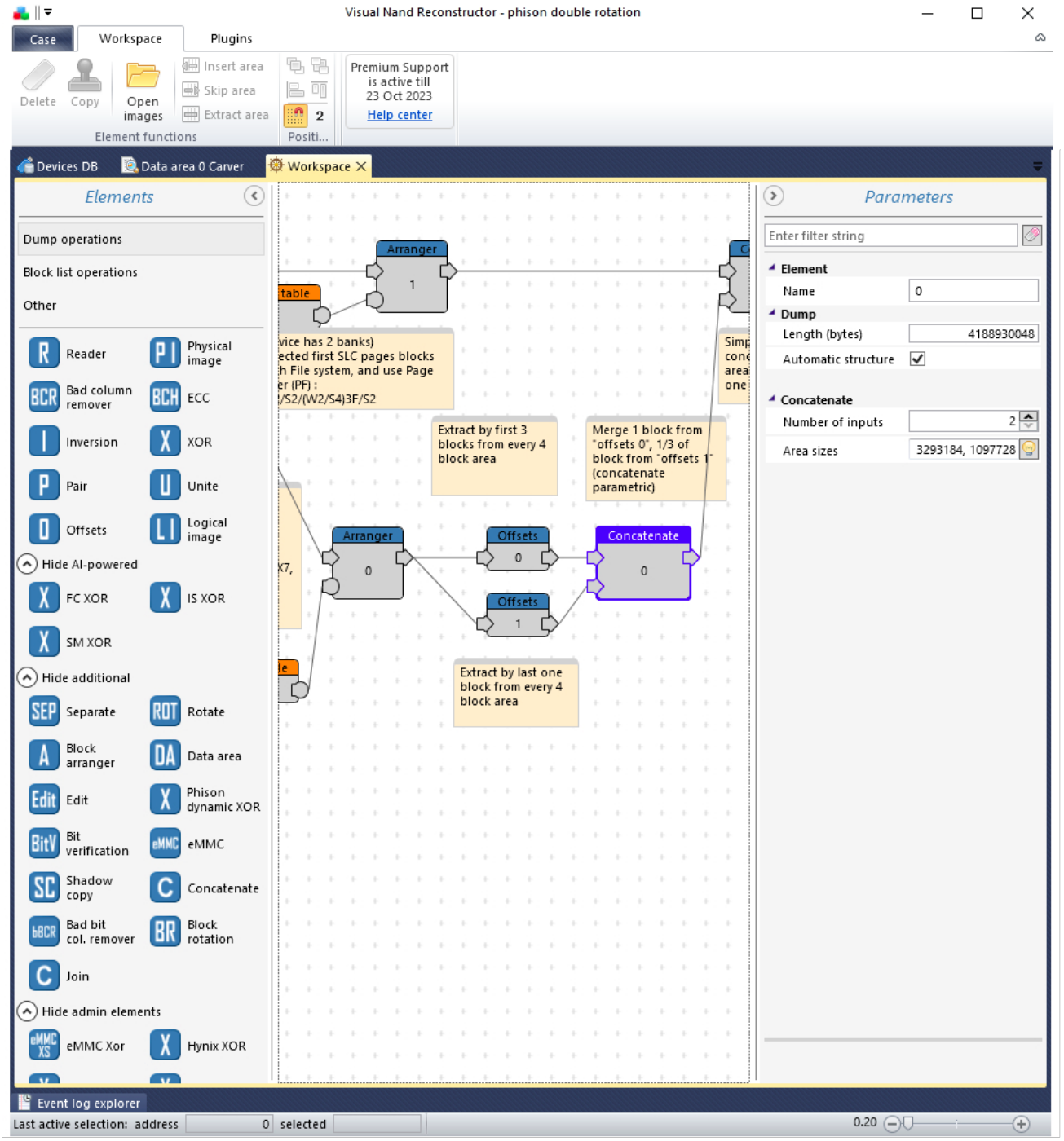
In the attached graphs there are also notifications with instructions to follow.



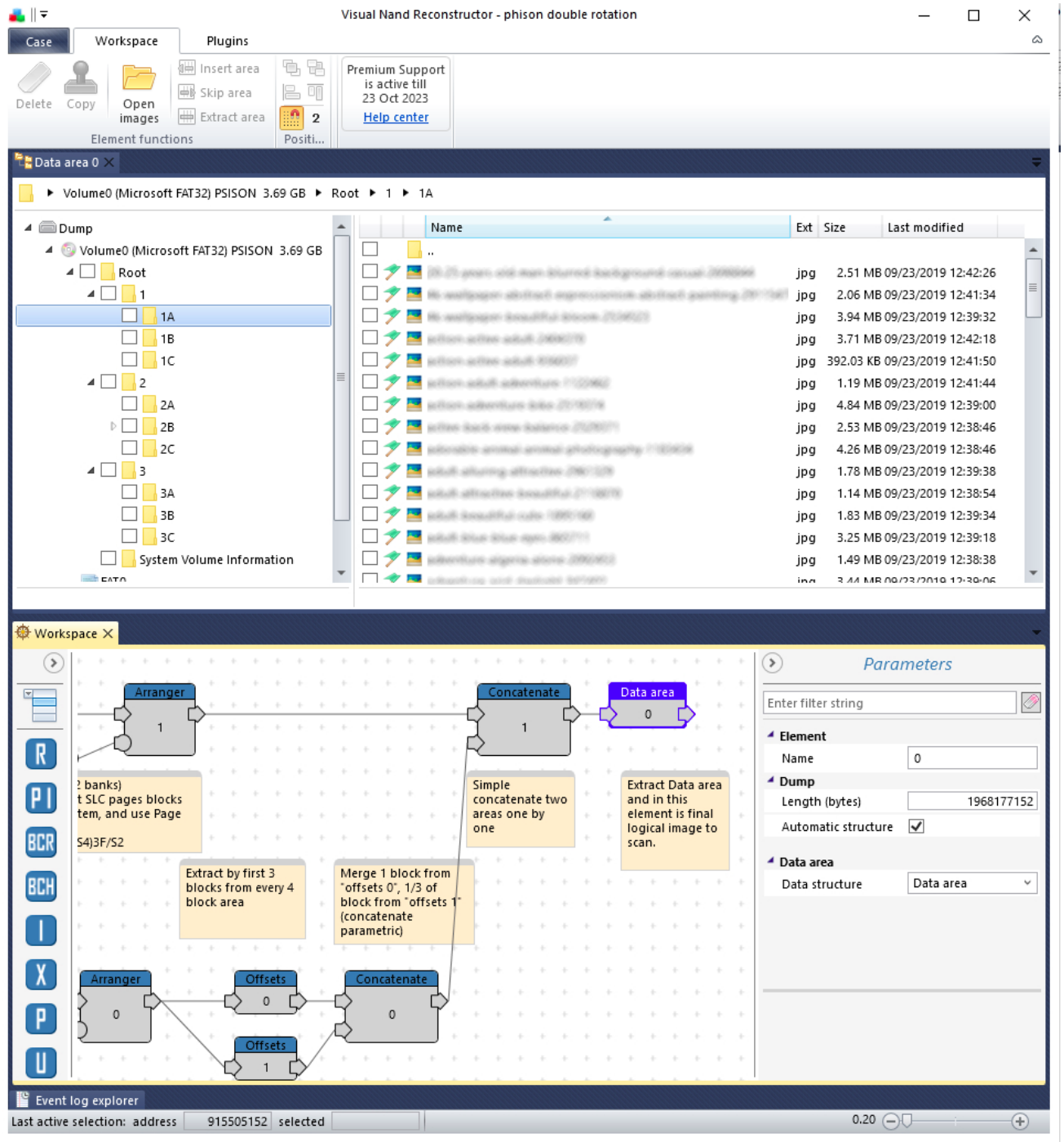
Sometimes, if there are two Banks, it is necessary to check the “Auto” flag and after that add 2 banks:



If all conditions are met, then the first parametric concatenate works correctly.



The second Concatenate is a simple concatenate by full areas, so it is necessary to just click the “bulb”. Then the fully recovered logical image will be in the Data area:



https://support.rusolut.com/portal/en/kb/articles/no-pic-no